Cybersecurity Incident Report: Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.
As part of the DNS protocol, the UDP protocol was used to contact the DNS server to retrieve an IP address. The ICMP protocol was used to respond with the error message “udp port 53 unreachable” indicating issues contacting the DNS server. It is highly likely that the DNS server is not responding.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.
The incident occurred today at 1:24 p.m. Customers notified the organization that they received the message “destination port unreachable” when they attempted to visit a website. The cybersecurity team providing IT services to their client organization are currently investigating the issue so customers can access the website again. In our investigation into the issue, we conducted packet sniffing tests using tcpdump. In the resulting log file, we found that DNS port 53 was unreachable. The next step is to identify whether the DNS server is down or traffic to port 53 is blocked by the firewall. The DNS server might be down due to a successful Denial of Service attack or a misconfiguration.